

NAMRATHA M

MFC5

BOOK-1

09-01-2018

MFC5

- ① Counting & Probability
- ② Logics - Proposition logic, Predicate logic
- ③ Algebra - Linear algebra - Basis, dimension, matrix, Group, Ring, Fields
- ④ Graph Theory
- ⑤ Complexity Theory - P & NP problems

BOOKS:

Discrete Mathematics - Kretz Rosen

" - C.L. Liu

Graphs - Narsingh Deo

COUNTING:

Two words

Product Rule  $m, n \rightarrow mn$

Sum Rule  $m, n \rightarrow m+n$

M. Tech 1 - 28 - 1 CR from 1 } 28 x 28 ways  
M. Tech 2 - 28 - 1 CR from 2 }

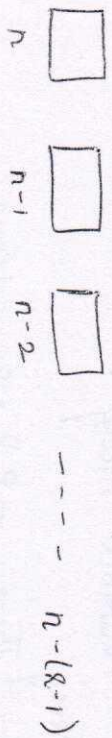
1 CR from both - 28 + 28 ways

Permutation:  $nPr$   $(n, r)$

Ordered arrangement of ' $r$ ' objects out of ' $n$ ' objects

a b c — 6 ways

a b c    b a c    c a b  
a c b    b c a    c b a



↓    ↓    ↓  
3 × 2 × 1 = 6 ways

$$nPr = \frac{n!}{(n-r)!}$$

$$= \frac{n \times (n-1) \times (n-2) \times \dots \times (n-(r-1)) \times (n-r)!}{(n-r)!}$$

$$= n!$$

Distribution of ' $x$ ' distinct objects into ' $n$ ' distinct cells.

Each cell can hold max. 1 object (no repetition)

5 class rooms  $\rightarrow$  4 classes =  $5P4$

$$5 \times 4 \times 3 \times 2 \times 1 = \underline{\underline{120}}$$

Suppose, each cell can hold any number of objects.

$$= n^r$$

(instead of 1)

(ordered collection of ' $r$ ' objects out of ' $n$ ' objects with repetition)

Ordered collection of 28 students ( $n = 28, r = 28$ )

$${}^{28}P_{28} = \underline{\underline{28!}}$$

Putting ' $n$ ' objects in a line —  $n!$

No. of ways of putting ' $n$ ' objects in a single

$$= n! = \underline{\underline{(n-1)!}}$$

All ' $n$ ' objects are treated as one single object

$$\left( \begin{matrix} n \\ x \end{matrix} \right) \left( \begin{matrix} n \\ x \end{matrix} \right)$$

10.01.2018

1. Different 9 digit nos are possible

1, 2, 3, ..., 9, 9

$${}^9P_9 = \underline{9!} \rightarrow \text{without repetition}$$

$$\underline{9^9} \rightarrow \text{with repetition}$$

Atleast one digit should be repeated

$$= \underline{9^9 - 9!}$$

Lemma: Let there be 'n' distinct objects  $q_1$  objects of one kind,  $q_2$  objects of 2nd kind, ...  
 $q_t$  objects of t-th kind  
 Permutation of 'n' objects =  $\frac{n!}{q_1! q_2! \dots q_t!}$

Proof:

Required answer = x

$q_1$  objects of one kind is changed to  $q_1$  distinct objects

$$\text{Required permutation} = x \times q_1!$$

Repeat the same for  $q_2 = x \times q_2!$

Repeat ... for all types of objects  
 $x \times q_1! \times q_2! \dots q_t! = \underline{x \cdot n!}$

$\rightarrow$  answer

$$x = \frac{n!}{q_1! q_2! \dots q_t!}$$

$\frac{(k!)!}{(k!)^{(k-1)!}}$  is a number or  $(k!)!$  is divisible by  $(k!)^{(k-1)!}$

$$\text{Suppose } n = k!, \quad \frac{n!}{(n!)^{(k-1)!}} = \frac{k!}{(k!)^{(k-1)!}}$$

$k!$  objects -  $k$  objects of 1st type,  $k$  objects of 2nd type, ...  $k$  objects of  $(k-1)$ -th type

$$= \frac{(k!)!}{k! k! \dots k! [(k-1)!] \text{ times}}$$

$\frac{\text{Numerator} - \text{number}}{\text{Denominator} - \text{number}}$  } since both are permutations

COMBINATIONS: Selection of 'x' objects out of 'n' distinct objects - no ordering

$${}^n C_x = \frac{n!}{(n-x)! x!}$$

$$nPr = \frac{n!}{(n-r)!}$$

Selecting 3 out of 26 alphabets  
DAB BAD DBA ABD BDA ADB

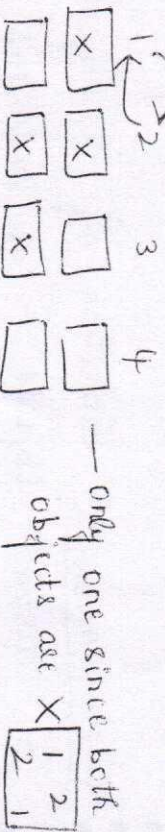
6 permutations -  $(3!) \Rightarrow 6$

This will be replaced by 1 when order is not required

$$nCr = \frac{n!}{(n-r)!r!}$$

Distribution of non-distinct objects into 'n' distinct cells  $\rightarrow nCr$  ( $r < n$ )

Putting 2 X (same X) into 4 distinct cells



$$= {}^4C_2$$

3 numbers are selected from 1, 2, 3, ..., 300 such that their sum is divisible by 3. How many ways

|   |   |   |   |           |
|---|---|---|---|-----------|
| ① | 3 | 6 | 9 | mod 3 = 0 |
| ② | 1 | 4 | 7 | mod 3 = 1 |
| ③ | 2 | 5 | 8 | mod 3 = 2 |

$$100C_3 + 100C_3 + 100C_3 + 100C_1 \times 100C_1 \times 100C_1$$

④ 1 number from category 1, 1 no from category 2 & 1 no from category 3

Other combinations of ①, ② & ③ are not possible such as 2 nos from ② & 1 no from ③

Number of different 32-bit sequence in which there is exactly seven 1's (rest are 0's).  
How many ways?

$${}^{32}C_7$$

Distribution of 7 (non-distinct) 1's into 32 cells

12.01.2018

Selection of 'x' objects out of 'n' distinct objects with repetition  $n+r-1 C_r$

Proof:

Distribution of 'x' non-distinct objects in ~~each~~ 'n' distinct cells in which each cell can hold any no of objects.

→ Represent using  $baa(1)$  and  $stars (*)$   
 $n=4$ ,  $(n-1) baas(1)$ ,  $r=6$

①  $* * | | | * * * *$

Interpretation: First object exists before first bar

Can also choose 'n' bars

1 | 2 | 3 | 4 | or 1 | 2 | 3 | 4

②  $* | * | * * *$

⑤  $* * * * * | |$

③  $* * | * * | * * |$

⑥  $||| * * * * *$

We have  $n-1$  bars,  $r$  stars  
 Ordered arrangement of 'n-1' bars & 'r' stars

$$= \frac{(n+r-1)!}{(n-1)! r!} \quad (\text{previous permutation formula})$$

①

$$x_1 + x_2 + x_3 + x_4 = 20$$

$x_i \geq 0$  (integer) — only integer solution

Distribution of 20 's' into 4 variables (cells)

$$= {}^{20+4-1}C_{20} = {}^{23}C_{20}$$

$$= \frac{23!}{20! 3!} = \frac{23 \times 22 \times 21 \times 20!}{20! \times 3 \times 2} = 23 \times 7$$

②

3 distinct dice are thrown — find the total no of possible outcomes?

Dice 1: 1 2 3 4 5 6  
 Dice 2: 1 2 3 4 5 6  $\Rightarrow 6^3$   
 Dice 3: 1 2 3 4 5 6

③

3 indistinguishable dice  $= 3+6-1 C_3 = 8C_3$

Distribution of 3 non-distinct (3 dice) into 6 cells (6 outcomes) in which each outcome can be repeated any no. of times.

$n=6, r=3$   
 $6+3-1C_3 = \underline{\underline{8C_3}}$

③ Distribute 7 apples & 5 oranges to 4 children  
 non-distinct  $\downarrow$  non-distinct

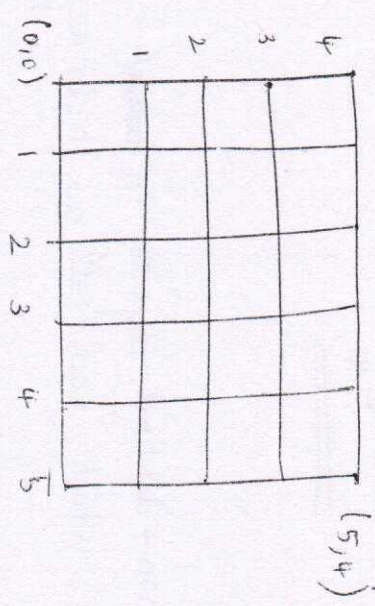
$r=7, n=4$   
 $4+7-1C_7$   
 $10C_7$   
 $r=5, n=4$   
 $5+4-1C_5$   
 $8C_5$

$10C_7 \times 8C_5$  (Product Rule)

Order of the objects within the cell is not considered here. (above examples)

Distribution of 'r' distinct objects into 'n' distinct cells where within the cell order of the objects matter.  
 $n \times (n+1) \times (n+2) \dots (n+r-1)$  ways

Distribution of 'r' non-distinct objects into 'n' non-distinct cells = One way (Trivial case)

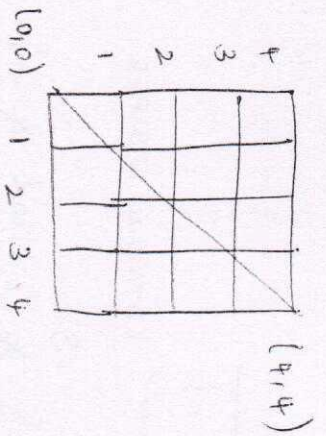


Go from (0,0) to (5,4) - total no. of paths  
 ① Without any restriction on number of paths  
 =  $\infty$

② Can move only East or North  
 $\begin{matrix} (0,0) & \xrightarrow{N} & (0,1) \\ & \searrow & \uparrow \\ & (1,0) & \end{matrix}$   
 East or North

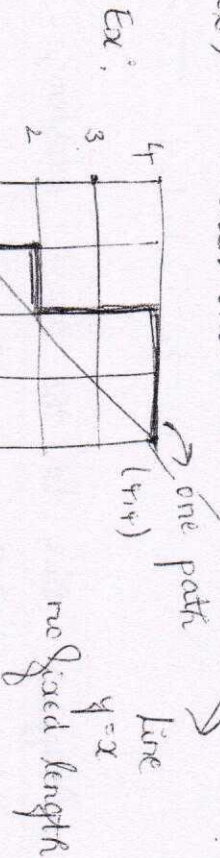
No. of paths is constant = 5  
 No. of paths is constant = 4  
 Path consists of total 9 steps  
 1-2-3-4-5  $\uparrow$  1-2-3-4-5  
 1-2-3-4  $\uparrow$  1-2-3-4

Arrangement of 9 steps in which 5 steps are East and 4 steps are North =  $9!$



direction movement allowed =  $\frac{(4+4)!}{4!4!}$

No of paths which crosses the line  $y=x$  (diagonal) - atleast once



Few Paths are:

- ① R U R U R R
- ② U U U U R R R R
- ③ R U U U R R U U R

Difficult to find paths  $\therefore$  Map to some other paths for which we can find solution

One-to-one mapping  $f: X \rightarrow Y$  (onto function)

Path ① R U U / R U U R R

↓ swap U & R

R U U / U R R U U

② U U U U / R R R R

↓ swap

U R R R U U U U

③ R U U U R R U R

↓ swap

R U U R U U R U

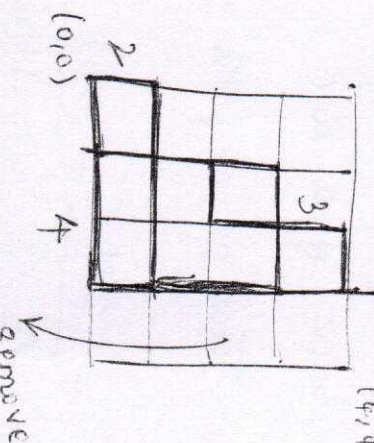
Swapping happens when no of U's exceeds the no of R's

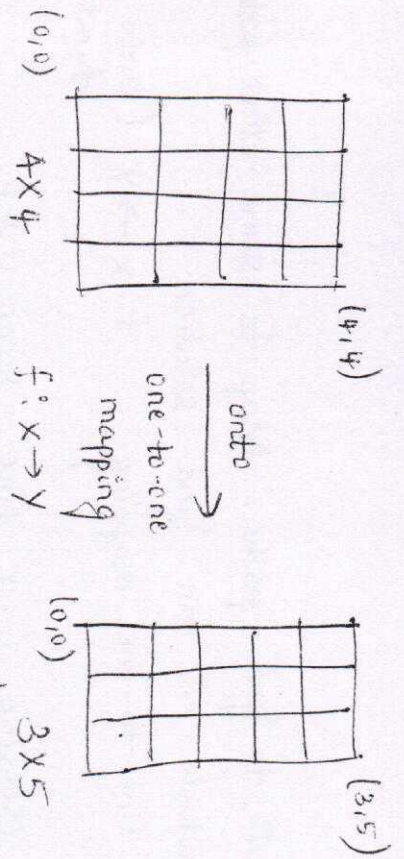
④ R R R U U U U / R

3 4

↓ swap

R R R U U U U U





No of paths from  $(0,0)$  to  $(3,5)$  in  $3 \times 5$  matrix

$$= \frac{8!}{3!5!}$$

In terms of 'n'  $= \frac{2n!}{(n-1)!(n+1)!}$

↓  
no of paths which crosses the line  $y=x$

No of paths from  $(0,0)$  to  $(n,n)$  which lie below  $y=x$  line CATALAN NUMBER

Total no of paths - No of paths which crosses the line  $y=x$

$$= \frac{2n!}{n!n!} - \frac{2n!}{(n-1)!(n+1)!} = \left[ \frac{1}{(n-1)!} - \frac{1}{n!} \right] \frac{2n!}{n!} = \frac{1}{n!} \cdot \frac{2n!}{n!n!}$$

$$= \frac{1}{(n+1)!} \cdot \frac{2n!}{n!n!} \quad \text{CATALAN NUMBER}$$

No of sequences of  $3$   $1$ 's and  $3$   $-1$ 's such that in any prefix no of  $-1$ 's does not exceed the no of  $1$ 's

For example:

1, -1, 1, -1, 1, -1  
1, 1, 1, -1, -1, -1  
1, 1, -1, -1, 1, -1  
1, -1, -1, 1, 1, -1

✓  
✗

Mapping this to the above problem,

$1 \rightarrow R, -1 \rightarrow U$

No of  $R$ 's  $\geq$  No of  $U$ 's

$$= \frac{1}{(3+1)!} \cdot \frac{(2 \cdot 3)!}{3!3!} = \frac{1}{4} \cdot 6C3$$

Matrix - Chain Multiplication - Dynamic Programming  
or Bate frae Method

3 matrices  $(A(BC))$  or  $((AB)C)$   
 4 matrices  $((((AB)C)D))$   
 $((AB)(CD))$

2 ways of parenthesis

No of ways of parenthesis (correlate to R's & V's)

and

in any

For 3 matrices

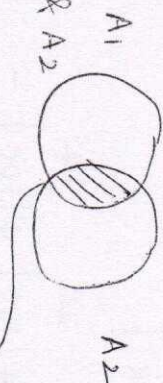
$$4C_2 = \frac{1}{2+1} \cdot \frac{4!}{2!2!} = \frac{4 \times 3 \times 2!}{2 \times 2! \times 2!}$$

For  $n$  matrices =  $\frac{1}{n} \cdot \frac{2(n-1)!}{(n-1)!(n-1)!}$   
 of ways  
 of parenthesisizing =  $\frac{1}{n} \cdot 2(n-1)C_{(n-1)}$   
 (not multiplying)

Brute force - Exponential time ( $\approx n^3$ )

# 17.01.2018

## Principles of Inclusion & Exclusion



$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

Generalization for 'n' events

$$\sum_{i=1}^n |A_i| = \sum_{1 \leq i_1 < \dots < i_n \leq n} |A_{i_1} \cap \dots \cap A_{i_n}|$$

$A_1$   $A_2$   
 and  
 $A_2$   $A_1$   
 are - to be  
 same - included  
 only once

$$+ \sum \left| A_{i_1 i_2 \dots i_{n+1}}^{i_1 i_2 \dots i_{n+1}} \right| A_{i_1 i_2 i_3}^{i_1 i_2 i_3} \dots$$

Can be proved using mathematical induction

Find the no of integers which are divisible by  $2^3, 5, 7$  and less than 100 ( $\leq 100$ ).

$$A_i = \text{set of integers divisible by } i$$

$$|A_2 \cup A_3 \cup A_5 \cup A_7| = |A_2| + |A_3| + |A_5| + |A_7|$$

$$= |A_2| + |A_3| + |A_5| + |A_7| + \dots + |A_{2n-1} \cap A_3| + \dots + |A_{2n-1} \cap A_{2n-3}|$$

$$(|A_2 \cap A_3 \cap A_5| + \dots)$$

$$|A_i| = \left\lfloor \frac{100}{i} \right\rfloor$$

$$|A_i \cap A_j| = \left\lfloor \frac{100}{i \cdot j} \right\rfloor$$

$$|A_i \cap A_j \cap A_k| = \left\lfloor \frac{100}{i \cdot j \cdot k} \right\rfloor$$

$$= \left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{3} \right\rfloor + \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{7} \right\rfloor -$$

$$- |A_2 \cap A_3 \cap A_5 \cap A_7|$$

$$\rightarrow = 0$$

No of primes  $\leq 100$

$$\sqrt{100} = 10$$

2, 3, 5, 7  $\rightarrow$  not divisible by any of these

$$\frac{|A_2 \cup A_3 \cup A_5 \cup A_7|}{100 - x} = 100 - x$$

$\neq 4$  (includes 1 because it is not divisible by 2, 3, 5, 7)

$$\text{No of primes} = 4 - 1 + 4$$

$$(1) (2, 3, 5, 7)$$

Derangement: Each of a set of object has a position that it is forbidden to occupy and no 2 objects have the same position. A derangement of these objects is a permutation of them such that no object is in its forbidden position.

$A_i$  =  $i$ th object is in its forbidden position

No of arrangements in which atleast one object is in its forbidden position =  $|A_1 \cup A_2 \cup \dots \cup A_n|$

$$\text{Derangement} = \underbrace{n!}_{\text{total no}} - |A_1 \cup A_2 \cup \dots \cup A_n| = |A_1 \cup A_2 \cup \dots \cup A_n|$$

sample space

$$|A_1 \cup A_2 \cup \dots \cup A_n| = \sum_{i=1}^n |A_i| - \sum_{i < j} |A_i \cap A_j| + \dots + (-1)^{n+1} |A_1 \cap A_2 \cap \dots \cap A_n|$$

$$+ \sum_{i < j < k} |A_i \cap A_j \cap A_k| + \dots + (-1)^{n+1} |A_1 \cap A_2 \cap \dots \cap A_n|$$

$|A_i| = (n-1)!$  - only one object is in its forbidden position, remaining objects can be placed anywhere

$$|A_i \cap A_j| = (n-2)!$$

$$|A_i \cap A_j \cap A_k| = (n-3)!$$

$$= nC_1 (n-1)! - nC_2 (n-2)! + nC_3 (n-3)! - \dots - (-1)^{n+1} nC_n \cdot \underbrace{(n-n)!}_{0!}$$

$\nearrow$  no. of terms  
 $\nearrow$  no. of terms

$$\text{Derangement} = n! - \left[ nC_1 (n-1)! - nC_2 (n-2)! + \dots - (-1)^{n+1} nC_n \cdot (n-n)! \right]$$

In how many ways can the letters  $\alpha, \alpha, \alpha, \alpha, \beta, \beta, \beta, \gamma, \gamma$  be arranged so that all the letters of the same kind are not in the same block? (not together)

$\gamma\beta\alpha\alpha\alpha\beta\beta\gamma$  - not allowed  
 $\alpha\alpha\beta\beta\gamma\gamma\beta\alpha$  - not allowed

$A_1$  = set of arrangements in which all  $\alpha$ 's are in the same block

$$A_2 = \beta$$

$$A_3 = \gamma$$

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3| - |A_1 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$

$$\text{Total} = \frac{9!}{1! 2! 1! 2!}$$

$$\text{arrangements} = \frac{4! 3! 2!}{1! 2! 1! 2!}$$

$$(2! 1! 1! 1!)$$

$$|A_1| = \frac{6!}{3! 2! 1!} \quad |A_2| = \frac{7!}{4! 2!} \quad |A_3| = \frac{8!}{4! 3!}$$

$$|A_1 \cap A_2| = \frac{4!}{2!}$$

$$|A_2 \cap A_3| = \frac{5!}{4!}$$

$$|A_1 \cap A_3| = \frac{5!}{3!}$$

$$|A_1 \cap A_2 \cap A_3| = 3! \quad (3 \text{ objects})$$

19.01.2018

Ex: 11 scientists are working on secret project. They wish to lock up the documents in a cabinet so that cabinet can be opened if and only if 6 or more scientists are present. What is the smallest number of locks needed? What is the smallest number of keys to the locks each scientist must have?

Solution:

5 person — 1 lock  
 No of locks = 11C5

Key of this lock is given

5 scientists together must not be able to open the lock - one more joins can open

5 persons together = 1 lock

Key to this lock is given to another 4 persons

10C5

or

11C5 - 10C4  
total choose remaining  
4 person

No of keys = 10C5

leave that person (11-1=10)

(Group of 5 where the scientist is not part)

Practically, not possible to carry so many locks and keys.

Shamir's Secret Sharing:

Secret (Number locking System - 2154) is

distributed to 'n' persons such that 't' or more person can compute the secret. (2154)  
Less than 't' persons cannot compute the secret.

Theorem:

Given 't' points  $(x_i, y_i)$ , ---  $(x_t, y_t)$  in the 2-D plane there is one and only one polynomial of degree  $t-1$  such that  $y_i = q(x_i)$ .

$$y = a + bx + cx^2 \rightarrow \text{polynomial}$$

Three unknowns - to solve 3 points are

required

< 3 cannot solve

$$y = 5 + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1}$$

↓ secret

$$(x_1, y_1) \rightarrow D_1$$

$$(x_2, y_2) \rightarrow D_2$$

↓

$$(x_n, y_n) \rightarrow D_n$$

Polynomial of degree  $t-1$   $\rightarrow$  leave  $x_1$  for  $a_1$

$$f(x) = a_1 \frac{(x-x_2) \dots (x-x_t)}{(x_1-x_2) \dots (x_1-x_t)} + a_2 \frac{(x-x_1)(x-x_3) \dots (x-x_t)}{(x_2-x_1) \dots (x_2-x_t)} + \dots + a_t \frac{(x-x_1) \dots (x-x_{t-1})}{(x_t-x_1) \dots (x_t-x_{t-1})}$$

Let  $x = x_1$   
 $y_1 = f(x_1) = a_1$  (other terms become 0)

$$y_2 = a_2$$

$$y_t = a_t$$

$$f(x) = y_1 \frac{(x-x_2) \dots (x-x_t)}{(x_1-x_2) \dots (x_1-x_t)} + y_2 \frac{(x-x_1)(x-x_3) \dots (x-x_t)}{(x_2-x_1) \dots (x_2-x_t)} + \dots + y_t \frac{(x-x_1) \dots (x-x_{t-1})}{(x_t-x_1) \dots (x_t-x_{t-1})}$$

Using 't' points we can compute  $f(x)$   
Secret  $S = f(0) = \text{constant term}$

$$f(x) = y_1 l_1(x) + y_2 l_2(x) + \dots + y_t l_t(x)$$

where  $l_i(x) = \frac{(x-x_1) \dots (x-x_{i-1})(x-x_{i+1}) \dots (x-x_t)}{(x_i-x_1) \dots (x_i-x_{i-1})(x_i-x_{i+1}) \dots (x_i-x_t)}$

$$f(0) = y_1 \frac{x_2 \dots x_t}{(x_2-x_1) \dots (x_t-x_1)} + \dots + y_t \frac{x_1 x_2 \dots x_{t-1}}{(x_{t-1}-x_1) \dots (x_{t-1}-x_{t-2})}$$

Secret

No need to use Kramér's rule to solve 'n' equations.

23.01.2018

### PROBABILITY

Measures the uncertainty.

Sample Size (Space) : Set of all possible outcomes

$$\text{Prob} = \frac{\text{No of outcomes}}{|S|}$$

Two coins:

$$SS = \{HH, HT, TH, TT\}$$

$$P(E \cup F) = P(E) + P(F) - P(E \cap F)$$

$$= \frac{n(E \cup F)}{|SS|}$$

Mutually Exclusive: E & F are mutually exclusive

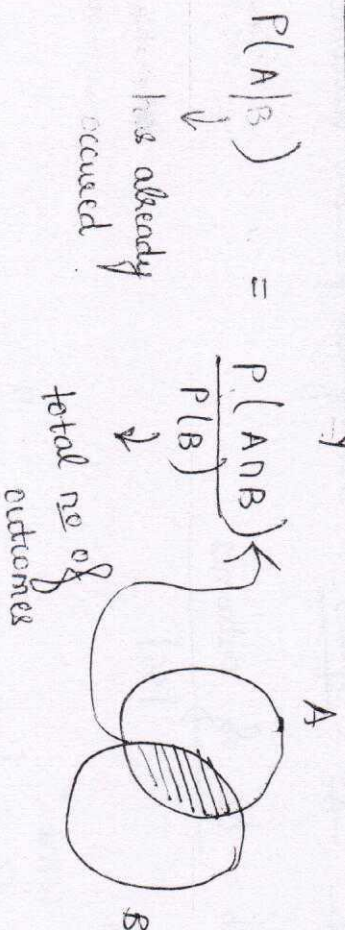
if  $E \cap F = \emptyset$   
 If one occurs, other doesn't occur.

$$E \cap E^c = \emptyset$$

$$P(E \cup E^c) = 1 = P(E) + P(E^c) - \underbrace{P(E \cap E^c)}_0$$

$$\boxed{P(E) + P(E^c) = 1}$$

Conditional Probability:



$$P(A|B) = \frac{n(A \cap B)}{n(B)}$$

$$= \frac{n(A \cap B) / n(S)}{n(B) / n(S)} = \frac{P(A \cap B)}{P(B)}$$

$$P(B|A) = \frac{P(B \cap A)}{P(A)} = \frac{P(A \cap B)}{P(A)}$$

$$P(B|A) \cdot P(A) = P(A|B) \cdot P(B) = P(A \cap B)$$

Independent Events:

$$P(A|B) = P(A)$$

↓  
 Occurrence of A doesn't depend on B

Mutually exclusive events are not independent events. (Highly dependent)

|           |                    |     |      |
|-----------|--------------------|-----|------|
| ① Husband | watches the show - | 80% | - H  |
| Wife      | " "                | 65% | - W  |
| Both      | " "                | 60% | - HW |

Find the probability that wife watches the show if husband watches the show

$$P(W|H) = \frac{P(W \cap H)}{P(H)} = \frac{60\%}{80\%} = \frac{3}{4} = 75\%$$

## Birthday Paradox:

How many person must be in a room before there is 50% chance that two of them are born on same day of the year?

$A_i$  = event that  $i$ th person's birthday is different from all  $j$ th person ( $j < i$ )

prob. that all  $K$  person have different birthday

$$P(A_1 | A_2 | A_3 \dots | A_K) = P(A | B) \cdot P(B)$$

or

$$P(B | A) \cdot P(A)$$

$$= P(A_K | A_1 | A_2 \dots | A_{K-1}) \cdot P(A_1 | A_2 \dots | A_{K-1})$$

$$= P(A_K | A_1 | A_2 \dots | A_{K-1}) \cdot P(A_{K-1} | A_1 | A_2 \dots | A_{K-2}) \cdot \dots$$

recursively apply conditional probability

$$= P(A_K | A_1 | A_2 \dots | A_{K-1}) \cdot P(A_{K-1} | A_1 | A_2 \dots | A_{K-2}) \cdot \dots$$

$$= P(A_K | A_1 | A_2 \dots | A_{K-1}) \cdot P(A_{K-1} | A_1 | A_2 \dots | A_{K-2}) \cdot \dots$$

$$= P(A_1) \cdot P(A_2 | A_1) \cdot P(A_3 | A_1 | A_2) \cdot \dots$$

$$= 1 \cdot P(A_K | A_1 | A_2 \dots | A_{K-1})$$

$$= \frac{N}{N} \cdot \left(\frac{N-1}{N}\right) \cdot \left(\frac{N-2}{N}\right) \cdot \dots \cdot \left(\frac{N-(K-1)}{N}\right)$$

$$= \frac{N}{N} \cdot \left(1 - \frac{1}{N}\right) \cdot \left(1 - \frac{2}{N}\right) \cdot \dots \cdot \left(1 - \frac{K-1}{N}\right)$$

$$\approx \exp\left(-\frac{(1+2+\dots+K-1)}{N}\right)$$

$$= \exp\left(-\frac{K(K-1)}{2N}\right)$$

$e^{-x} \approx 1-x$  for small

Prob. that atleast 2 person out of  $K$  have same birthday =  $1 - \exp\left(-\frac{K(K-1)}{2N}\right)$

$$1 - \exp\left(-\frac{K(K-1)}{2N}\right) \approx \frac{1}{2}$$

already given

$$K = 1.17 \sqrt{N}$$

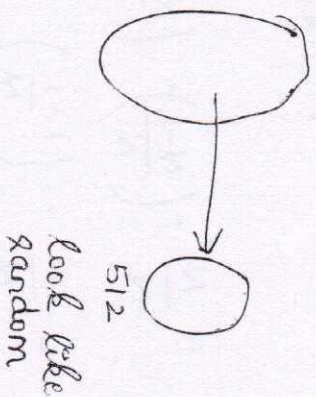
$\rightarrow 365$

$\approx 23$

Application: Hash Function in Cryptography

$$H: \{0,1\}^* \xrightarrow{\text{SHA-512}} \{0,1\}^{512}$$

any arbitrary string  
( $\ggg 512$ )



$$\exists x_1, x_2 \\ H(x_1) = H(x_2)$$

If should be hard to find  $x_1$  and  $x_2$  such that  $H(x_1) = H(x_2)$  — collision resistant property

$$\text{Message Digest} = M = 2^{512}$$

$$\text{Worst case: } O(\underbrace{2^{512}}_N) - \text{collision occurs}$$

$$\begin{aligned} H(x): & \text{ Birthday of } x \\ H(x_1): & \text{ " } x_1 \\ H(x_2): & \text{ " } x_2 \end{aligned}$$

In  $\sqrt{N}$  trials — with probability  $= 1/2$  or 50% one can find the collision

$$O(\underbrace{2^{512}}_N) \implies O(\sqrt{2^{512}}) = O(2^{256})$$

$$\text{prob} = 1/2$$

24.01.2018

Ex: Each of three men at a party throws their hat into the centre of the room, hats are mixed up. Then each man randomly selects one hat. What is the probability that none of the three men selects his own hat?

Similar to derangement.

$$\begin{aligned} \text{No. of ways none of 3 men selects his own hat} \\ &= 3! - 3C_1 \cdot 2! + 3C_2 \cdot 1! - 3C_3 \cdot 0! \\ &= 6 - 3 \times 2 + 3 - 1 = \underline{\underline{2 \text{ ways}}} \end{aligned}$$

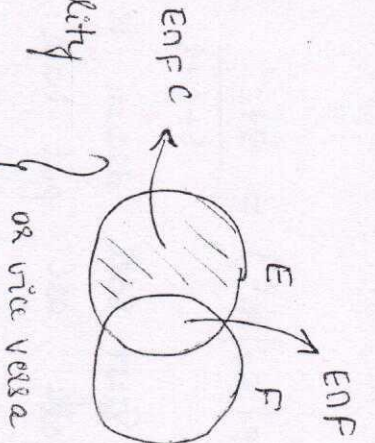
$$\text{Probability} = \frac{2}{3!} = \frac{2}{6} = \frac{1}{3}$$

OR  
find  $P(\text{AUBUC}) \xrightarrow{3 \text{ hats}}$   
Answer:  $1 - P(\text{AUBUC})$

## Bayes Theorem:

$E/F$  : Prior Probability (known)

$F/E$  : Posterior Probability (to find)



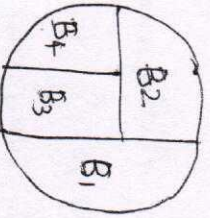
$$E = (ENF) \cup (ENFc)$$

$$P(E) = P(ENF) + P(ENFc) = P(ENF) + P(ENFc) \cdot P(Fc)$$

$$P(E) = P(E|F) \cdot P(F) + P(E|Fc) \cdot P(Fc)$$

$$= P(E|F) \cdot P(F) + P(E|Fc) \cdot P(Fc)$$

$$P(F|E) = \frac{P(ENF)}{P(E)} = \frac{P(E|F) \cdot P(F)}{P(E|F) \cdot P(F) + P(E|Fc) \cdot P(Fc)}$$



$B_1, B_2, B_3, B_4$  - positions of  $E$

$$\cup B_i = E \quad \& \quad B_i \cap B_j = \emptyset$$

$$P(B_i|E) = \frac{P(B_i \cap E)}{P(E)} = \frac{P(E|B_i) \cdot P(B_i)}{P(E)}$$

\* Probability model - Seldon Ross (Exercise 1 FIRST 2 CHAPTERS) Problems)

$$= \frac{P(E|B_1) \cdot P(B_1)}{P(E|B_1) \cdot P(B_1) + P(E|B_2) \cdot P(B_2) + P(E|B_3) \cdot P(B_3) + P(E|B_4) \cdot P(B_4)}$$

$$E = (ENB_1) \cup (ENB_2) \cup (ENB_3) \cup (ENB_4)$$

Ex: ① A laboratory is 95% effective in detecting a certain disease when in fact disease. However the test also yields a false positive result for 1% of the healthy person tested. If 8.5% of the population actually has the disease, what is the probability a person has the disease given that his test result is positive.

$D \rightarrow$  person has the disease  
 $P \rightarrow$  test result is positive

$$P(D|P) = \frac{P(P|D) \cdot P(D)}{P(P|D) \cdot P(D) + P(P|Dc) \cdot P(Dc)}$$

$$= \frac{0.95 \times 0.005}{0.95 \times 0.005 + 0.01 \times 0.995}$$

(Urn)

② Container contains 'b' ~~black~~ balls & 'r' red balls.

One of the ball is drawn at random but while it is put back in the urn 'c' additional balls of the same color are put in with it. Now suppose that we draw another ball so that the probability that the first ball drawn was black given that second ball drawn is red.

$B_1 \rightarrow$  first ball drawn was black  
 $R_2 \rightarrow$  second ball drawn is red

$$P(B_1|R_2) = \frac{P(R_2|B_1) \cdot P(B_1)}{P(R_2|B_1) \cdot P(B_1) + P(R_2|B_1^c) \cdot P(B_1^c)}$$

$$P(B_1) = \frac{b}{b+r}$$

$$P(B_1^c) = 1 - \frac{b}{b+r} = \frac{r}{b+r}$$

$$P(R_2|B_1) = \frac{r}{b+c+r}$$

First ball drawn is black, while putting back - c additional black balls are put in.

$$P(R_2|B_1^c) = \frac{r+c}{b+c+r}$$

If first ball drawn is red, 'c' additional red balls are put back.

$$P(B_1|R_2) = \frac{\frac{r}{b+c+r} \cdot \frac{b}{b+r}}{\frac{r}{b+c+r} \cdot \frac{b}{b+r} + \frac{r+c}{b+c+r} \cdot \frac{r}{b+r}}$$

$$= \frac{\cancel{r} \cdot b}{(b+r)(b+c+r)} + \frac{r(r+c)}{(b+c+r)(b+r)} \\ = \frac{br}{br+r^2+rc} = \frac{b}{b+r+c}$$

30.01.2018

ELT: transmit the signal. The Altigauge (A) manufacturing company makes 80% of ELT & B company makes 15% & C company makes 5%. The ELT made by A has 4% defects, B has 6% defects & C has 9% defects. If a random ELT is

tested and is found to be defective, find the probability that it is made by A.

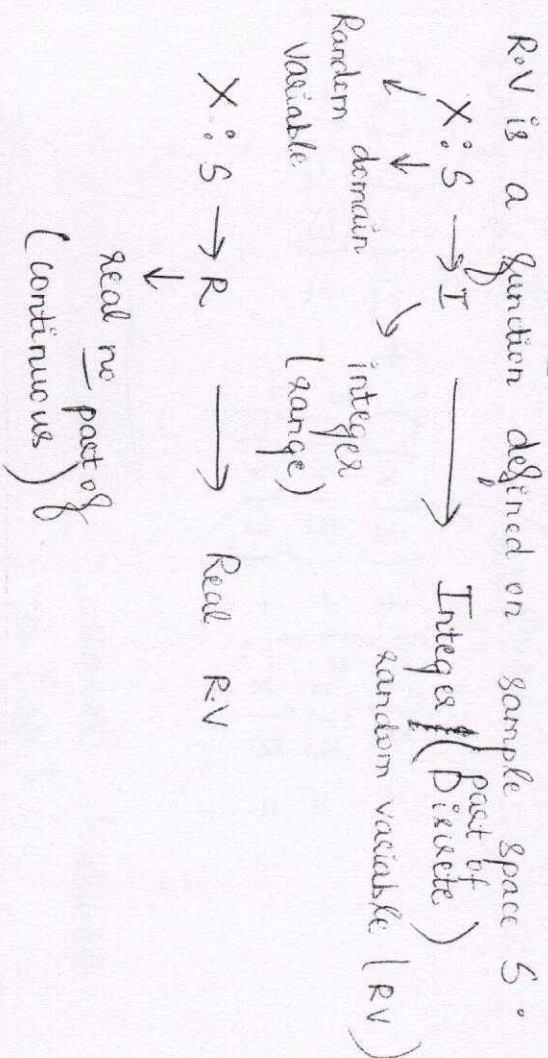
A: Selected ETR is found to be defective  
 B<sub>1</sub>: ETR is made by A company

$$P(B_1|A) = \frac{P(A|B_1) \cdot P(B_1)}{P(A|B_1) \cdot P(B_1) + P(A|B_2) \cdot P(B_2) + P(A|B_3) \cdot P(B_3)}$$

$$= \frac{0.04 \times 0.8}{0.04 \times 0.8 + 0.06 \times 0.15 + 0.09 \times 0.05}$$

### RANDOM VARIABLES:

R.V is a function defined on sample space S.



Ex: Two coins are tossed.  $S = \{HH, HT, TH, TT\}$   
 let X be a RV which denotes no. of heads.

$X: S \rightarrow \{0, 1, 2\}$

$$P[X=0] = \frac{1}{4} \quad (\text{Only TT occurs})$$

$$= P(0) \quad \text{no of heads} = 0$$

↓  
 Probability Mass function (PMF)

$$\boxed{\sum_i P(i) = 1}$$

Discrete - PMF (Mass)  
 Continuous - PDF (Density) Density = Mass/Area

Cumulative Distribution Function (CDF)

$$F(a) = \sum_{i \leq a} P(i)$$

Bernoulli's Distribution: (Part of discrete random variable)

$X: S \rightarrow C$  (countable set)

I is part of C [ICC]

Two possible outcomes: — Success (p) S=1  
Failure (1-p) F=0

$$X: S \rightarrow \{0, 1\}$$

$$P[X=1] = p = P(1)$$

$$P[X=0] = (1-p) = P(0)$$

$$E[X] = \text{expected value of RV } X \\ = \frac{1 \cdot P(1) + 0 \cdot P(0)}{P + (1-p)} = P(1) = p$$

$$\therefore E[X] = p \quad (\text{same as probability of success})$$

$$\text{Variance (measure of spreadness)} \\ = E[X - E[X]]^2$$

(Squaring done in order to make sure that +ve & -ve terms don't cancel out)

To compute Variance:

① Find expected value

② Subtract from each value

Square all values

Sum up the values

$$X: S \rightarrow \{x_1, x_2, x_3\}$$

Variance =

$$P(x_1)(x_1 - E[X])^2 + P(x_2)(x_2 - E[X])^2 + P(x_3)(x_3 - E[X])^2$$

$$\text{Variance} = E[X - E[X]]^2 \\ = E[X]^2 + (E[X])^2 - 2 \cdot X \cdot E[X]$$

$$= E[X]^2 + E[(E[X])^2] - E[2X E[X]]$$

$$① E[CX] = CE[X]$$

constant

$$② E[C] = C$$

using this

using this

$$= E[X^2] + (E[X])^2 + 2E[X]E[X] \\ = E[X^2] + (E[X])^2 - 2(E[X])^2 \\ = E[X^2] - (E[X])^2 \\ = \sigma^2$$

Standard

Deviation =

$$\sqrt{\text{Variance}}$$

$$(SD) \sigma$$

Variance for Bernoulli's distribution:

$$E[X] = p$$

$$E[X^2] = \frac{x_1^2 p(x_1) + x_2^2 p(x_2)}{p}$$

$$= \frac{1^2 \cdot p + 0^2 \cdot (1-p)}{p}$$

$$\text{Variance} = E[X^2] - (E[X])^2 = p - p^2 = \underline{p(1-p)}$$

21.01.2018

Geometric RV:

Ex: Probability that 10th time - first head

$$\underbrace{\left(\frac{1}{2}\right)^9}_{9 \text{ times we get Tail}} \cdot \frac{1}{2}$$

All trials here are independent of each other.

Independent trials and each trial has 2 possibilities  $p(\text{success})$  and  $(1-p)(\text{failure})$

X: (RV)

Number of trials required until first success comes

$$X: S \rightarrow \{1, 2, \dots, \infty\}$$

$$P[X=n] = p(1-p)^{n-1} \cdot p$$

we may not get success

$n-1$  failures to get success in  $n$ th trial

$$E[X] = 1 \cdot p(1) + 2 \cdot p(2) + \dots + i \cdot p(i) + \dots$$

$$= \sum_{i=1}^{\infty} i \cdot p(i)$$

$$= \sum_{i=1}^{\infty} \underbrace{i(1-p)^{i-1}}_{\substack{\uparrow \\ \text{swap}}} \cdot p$$

$$= -p \sum_{i=1}^{\infty} \frac{d}{dp} (1-p)^i$$

swap

$$= -p \cdot \frac{d}{dp} \sum_{i=1}^{\infty} (1-p)^i$$

$$GP(\text{till } \infty) = \frac{a(r^{n-1})}{a-1}$$

$$= -p \cdot \frac{d}{dp} \frac{1-p}{1-(1-p)} = -p \frac{d}{dp} \left( \frac{1}{p} \right) = \frac{1}{p}$$

## Binomial Distribution:

'n' independent trials (already given) with 2 possibilities  $p$  &  $(1-p)$

Ex: Prob. of getting 5 heads in 10 trials.

$${}^{10}C_5 \cdot \left(\frac{1}{2}\right)^5 \cdot \left(\frac{1}{2}\right)^4$$

$\downarrow$  success       $\downarrow$  failure

X: Denotes the number of successes in n-trials

$$X: S \rightarrow \{0, 1, 2, \dots, n\}$$

In n-trials we may not get any success at all.

$$P[X=0] = P(n) = {}^nC_0 \cdot p^0 \cdot (1-p)^{n-0}$$

$$E[X] = 0 \cdot P(0) + 1 \cdot P(1) + \dots + n \cdot P(n)$$

$$= \sum_{i=0}^n i \cdot P(i)$$

$$= \sum_{i=0}^n i \cdot {}^nC_i \cdot p^i \cdot (1-p)^{n-i} \quad (\text{When } i=0, \text{ term becomes } 0)$$

$$= \sum_{i=0}^n i \cdot {}^nC_i \cdot p^i \cdot (1-p)^{n-i}$$

$$= \sum_{i=1}^n i \cdot \frac{n(n-1)!}{(n-i)!i!} \cdot p \cdot p^{i-1} \cdot (1-p)^{n-i}$$

$$= np \sum_{i=1}^n \frac{i \cdot (n-1)!}{(n-i)!i!} \cdot p^{i-1} \cdot (1-p)^{n-i}$$

$$= np \sum_{i=1}^n \frac{(n-1)!}{\frac{(n-i)!}{i} (i-1)!} \cdot p^{i-1} \cdot (1-p)^{n-i}$$

$$= np \sum_{i=1}^n (n-1)C_{i-1} \cdot p^{i-1} \cdot (1-p)^{n-i}$$

$$= np \sum_{i=0}^{n-1} (n-1)C_i \cdot p^i \cdot (1-p)^{n-1-i} \quad (\text{Here } i-1=i)$$

Rewrite in this form of binomial distribution from 0 to n-1

$$= np \cdot (p + (1-p))^{n-1}$$

$$= np \cdot (1)^{n-1}$$

$$= np$$

Ex: An aeroplane engine will fail when in flight with probability  $(1-p)$ . Suppose that aeroplane will make successful flight if atleast 50% of its engines remain operative. For what value of  $p$  is a 4-engine plane

is preferable to 2-engine plane.

Probability that 4-engine plane will have a successful flight.

$$P[X \geq 2] = {}^4C_2 \cdot p^2 (1-p)^2 + {}^4C_3 \cdot p^3 (1-p)^1 + {}^4C_4 \cdot p^4 (1-p)^0$$

50% of 4

Probability that 2-engine plane will be successful

$$P[X \geq 1] = {}^2C_1 \cdot p^1 (1-p)^1 + {}^2C_2 \cdot p^2 (1-p)^0$$

50% of 2

$$4 {}^2C_2 \cdot p^2 \cdot (1-p)^2 + 4 {}^3C_3 \cdot p^3 (1-p)^1 + 4 {}^4C_4 \cdot p^4 (1-p)^0$$

$$> 2 {}^2C_1 \cdot p^1 (1-p)^1 + 2 {}^2C_2 \cdot p^2 (1-p)^0$$

$$6p^2(1+p^2-2p) + 4p^3(1-p) + p^4 > 2p(1-p) + p^2$$

$$6p^2 + 6p^4 - 12p^3 + 4p^3 - 4p^4 + p^4 > 2p - 2p^2 + p^2$$

$$3p^4 - 8p^3 + 6p^2 > -p^2 + 2p$$

$$3p^4 - 8p^3 + 7p^2 > 2p$$

$$3p^3 - 8p^2 + 7p > 2$$

## Negative Binomial Distribution:

Toss a coin until 'k' heads occur. What is the probability that it will happen in 15th trial?

$${}^{14}C_5 \cdot \left(\frac{1}{2}\right)^5 \left(\frac{1}{2}\right)^9 \cdot \frac{1}{2}$$

$${}^{n-1}C_{x-1} \cdot p^{x-1} (1-p)^{n-x} \cdot p$$

↓  
x - no of successes

First kind x-1 successes in n-1 trials & 1 success in nth trial.  
(no of successes) x → constant

no of trials → to find } similar to geometric RV

But in binomial, no of trials → fixed

To find → no of successes

## Examples

Negative Binomial is reverse of binomial

Binomial: No of successes given n trials

Negative Binomial: No of trials required for

$$P[X=n] = n-1 C_{n-1} p^{n-1} (1-p)^{n-1-(n-1)} \cdot p$$

No. of failures required for  $r$ -success.

$$P[X=r] = r-1 C_{r-1} p^{r-1} (1-p)^{(r-1)-(r-1)} \cdot p$$

$r \rightarrow$  no of success  
 $r \rightarrow$  no of failures  
 } Total:  $r+r$  trials

$$E[X] = \frac{r}{p}$$

### Hyper Geometry:

Consider a population of  $N$  individuals out of which  $K$  are male and  $N-K$  are female. A sample of  $n$ -individuals are randomly selected from this sample  $N$ . What is the probability that  $x$  males were selected?

$$n C_x \cdot \frac{N-K}{N} \cdot \frac{N-K-1}{N-1} \dots \frac{N-K-x+1}{N-x+1}$$

$K$  male -  $x$  males are selected  
 $\rightarrow$  total no of samples  
 $\rightarrow$  remaining female

$X$

HG RV: denotes no of males from the sample of  $n$

$$P[X=x] = \frac{n C_x \cdot \frac{N-K}{N} \cdot \frac{N-K-1}{N-1} \dots \frac{N-K-x+1}{N-x+1}}{N C_n}$$

$$E[X] = \frac{Kn}{N}$$

$$\text{Variance} = \frac{Kn(N-K)(N-n)}{N^2(n-1)}$$

Binomial Distribution:

$$P[X=r] = n C_r \cdot p^r (1-p)^{n-r}$$

$$\text{Average} = np = \lambda$$

As  $n \rightarrow \infty$  and  $r \rightarrow 0$  (very small)

$$P[X=r] = \frac{n!}{(n-r)! r!} \left(\frac{\lambda}{n}\right)^r \left(\frac{1-\lambda/n}{(1-\lambda/n)^n}\right)^{n-r} \rightarrow \frac{1}{r!} \lambda^r e^{-\lambda}$$

since  $n$  is large

$$= \frac{n!}{(n-r)! r!} \cdot \frac{\lambda^r}{n^r} \cdot \frac{e^{-\lambda}}{(1-\lambda/n)^{n-r}} \approx \frac{n!}{n^r} \cdot \frac{\lambda^r}{r!} \cdot e^{-\lambda}$$

$$= \left[ \frac{n}{n} \cdot \frac{n-1}{n} \cdot \frac{n-2}{n} \cdots \frac{n-(r-1)}{n} \right] \cdot \frac{e^{-\lambda} \lambda^r}{r!}$$

$$= \left[ \frac{n}{n} \cdot \left( \frac{n-1}{n} \right) \cdot \left( \frac{n-2}{n} \right) \cdots 1 - \frac{(r-1)}{n} \right] \cdot \frac{e^{-\lambda} \lambda^r}{r!}$$

$$= \frac{e^{-\lambda} \lambda^r}{r!}$$

↓  
Poisson Distribution

each term  $\approx 1$  since  
'n' is very large

Poisson RV: Denotes the no. of successes

$$P[X=r] = \frac{e^{-\lambda} \lambda^r}{r!}$$

All trials are random and independent.

$n \rightarrow \infty$  and  $p \rightarrow 0$   
↓  
no. of trials is very large → no. of successes is very low.

Arrival rate in a network - Poisson

No. of packets - very large ( $N \rightarrow \infty$ )  
Packets arrive in a particular network with probability  $p \rightarrow 0$  (very low since these are several networks)

Probability that 'x' packets arrive in a network (NIT) =  $\frac{e^{-\lambda} \cdot \lambda^x}{x!}$

Arrival of cars in Toll booth.

$N =$  no. of cars - very large  
 $p \rightarrow 0$  - because car arriving at a particular toll booth is very low (since there are many toll booths)

$$E[X] = \sum_{r=0}^{\infty} \frac{r \cdot e^{-\lambda} \lambda^r}{r!}$$

(  $r \cdot p_r$  )  
↓  
0 to  $\infty$  → probability

$$= \lambda \sum_{r=0}^{\infty} \frac{r \cdot e^{-\lambda} \lambda^{r-1}}{r!}$$

$$= \lambda e^{-\lambda} \sum_{r=0}^{\infty} \frac{r \cdot \lambda^{r-1}}{r!}$$

$$= \lambda e^{-\lambda} \sum_{r=1}^{\infty} \frac{r \cdot \lambda^{r-1}}{r!}$$

[  $r=0$  the whole term becomes 0 ]

$$= \lambda e^{-\lambda} \sum_{r=1}^{\infty} \frac{\lambda \cdot \lambda^{r-1}}{(r-1)!}$$

$$= \lambda e^{-\lambda} \sum_{r=1}^{\infty} \frac{\lambda^{r-1}}{(r-1)!}$$

$$\text{Let } x-1 = 1$$

$$= \lambda e^{-\lambda} \sum_{j=0}^{\infty} \frac{\lambda^j}{j!}$$

$$= \lambda e^{-\lambda} \left[ \frac{\lambda}{1!} + \frac{\lambda}{2!} + \dots + \frac{\lambda}{\infty!} \right]$$

$$= \lambda e^{-\lambda} \cdot e^{\lambda}$$

$$= \underline{\underline{\lambda}}$$

→ expected value

07.02.2018

Case (a) arrive at Toll Booth at average rate of 150 per hour. Find the probability that in a given minute no cars arrive.

(b) Probability that in a given minute 3 cars arrive.

Average of cars in a minute

Average rate =  $\frac{150}{60}$  per minute =  $\lambda$

$$[a] P[X=0] = \frac{\lambda^0}{0!} e^{-\lambda} = e^{-\lambda}$$

$$(b) P[X=3] = \frac{\lambda^3}{3!} \cdot e^{-\lambda} = \frac{\lambda^3}{6} \cdot e^{-\lambda}$$

(c) Probability that atleast 2 cars arrive

$$= 1 - P[X=0] - P[X=1]$$

$$= 1 - e^{-\lambda} - \lambda \cdot e^{-\lambda}$$

$$= \underline{\underline{1 - e^{-\lambda} (1 + \lambda)}}$$

Reception desk receives phone calls at the rate of 4 calls per 10 minutes. Assume that calls are random and independent with constant average rate. What is the probability of receiving no calls in a 5 minute period?

$$\lambda = 4 \text{ calls} / 10 \text{ minutes}$$

$$\lambda = 2 \text{ calls} / 5 \text{ minutes}$$

$$P[X=0] = \frac{e^{-\lambda} \cdot \lambda^0}{0!} = e^{-\lambda} = \underline{\underline{e^{-2}}}$$

## CONTINUOUS RANDOM VARIABLE:

$X: S \rightarrow R$  (continuous)

$$P[X=i] = P(i) = \text{point probability} = 0$$

infinite points

$\therefore$  We can't use  $P(i)$  here as in discrete RV.

$$f(x) = \frac{\text{Probability}}{\text{Density Function (PDF)}}$$
$$P[X=i] = 0 = P(i)$$

$$P[a \leq X \leq b] = \int_a^b f(x) dx$$

Point probability:

$$P[a \leq X \leq a] = \int_a^a f(x) dx = 0$$

Cumulative Distribution Function:

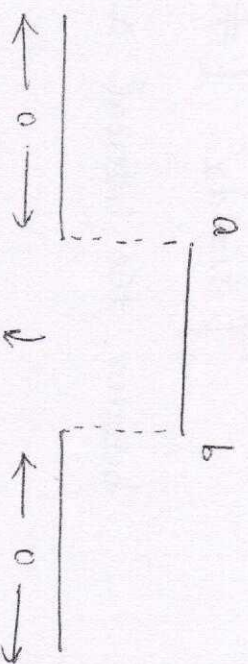
$$F[a] = \int_{-\infty}^a f(x) dx$$

$$\frac{d}{da} F[a] = f(a)$$

CDF

PDF

## 1. Uniform Random Variable:



R.V  $X$  is uniformly distributed  $a \leq X \leq b$

$$f(x) = \begin{cases} 0 & x \leq a \\ \frac{1}{b-a} & a \leq x \leq b \\ 0 & x \geq b \end{cases}$$
$$= \int_a^b \frac{1}{b-a} dx = \frac{1}{b-a} (b-a) = 1$$

Expected Value  $E[X]$

$$= \int_{-\infty}^{\infty} x f(x) dx$$

$$= \int_{-\infty}^{\infty} x f(x) dx$$

$$= \int_{-\infty}^a x f(x) dx + \int_a^b x f(x) dx + \int_b^{\infty} x f(x) dx$$

$$= \int_a^b x f(x) dx + \int_b^{\infty} x f(x) dx$$

$$\left\{ \begin{array}{l} \text{Expected value } E[X] = \int_a^c x f(x) dx \\ \frac{\int_a^c f(x) dx}{\int_a^c f(x) dx} \quad (\neq 1) \\ \text{between the interval } a \text{ to } c \end{array} \right.$$

$$\begin{aligned} &= \int_a^b x f(x) dx \\ &= \int_a^b x \cdot \frac{1}{b-a} dx = \frac{1}{b-a} \int_a^b x dx \\ &= \frac{1}{b-a} \left[ \frac{x^2}{2} \right]_a^b = \frac{(b-a)(b+a)}{(b-a)^2} \\ &= \frac{1}{b-a} \left[ \frac{b^2 - a^2}{2} \right] = \frac{(b-a)(b+a)}{(b-a)^2} \end{aligned}$$

$$\therefore E[X] = \frac{a+b}{2}$$

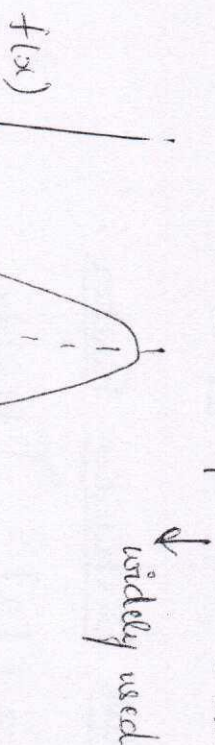
$$\text{Variance} = E[X - \mu]^2$$

↓  
expected value

$$\begin{aligned} &= \int_{-b}^b (x - \mu)^2 f(x) dx \\ &= \int_{-b}^b (x - \mu)^2 \cdot \frac{1}{1-b} dx \end{aligned}$$

$$\begin{aligned} &= \frac{1}{b-a} \int_a^b (x^2 + \mu^2 - 2\mu x) dx \\ &= \frac{1}{b-a} \int_a^b \left[ x^2 + \left(\frac{b+a}{2}\right)^2 - 2\left(\frac{b+a}{2}\right)x \right] dx \\ &= \frac{1}{b-a} \left\{ \left[ \frac{x^3}{3} \right]_a^b + \left(\frac{b+a}{2}\right)^2 x - 2\left(\frac{b+a}{2}\right)\left(\frac{x^2}{2}\right) \right\} \\ &= \frac{1}{b-a} \left[ \left(\frac{b^3 - a^3}{3}\right) + \left(\frac{b+a}{2}\right)^2 b - \cancel{2} \left(\frac{b+a}{2}\right) \left(\frac{b^2 - a^2}{2}\right) \right] \\ &= \frac{(b-a)^2}{12} \end{aligned}$$

2. Normal Distribution : (Gaussian Distribution)



Symmetric about the line  $x = \mu$

$$f(x) = \frac{1}{\sqrt{2\pi}\sigma} \cdot e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

$\downarrow$  SD                       $\nearrow$  mean

Ex: Marks distribution of students is normally distributed

$$\int_{-\infty}^{\infty} f(x) dx = 1$$

$$= \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}} dx$$

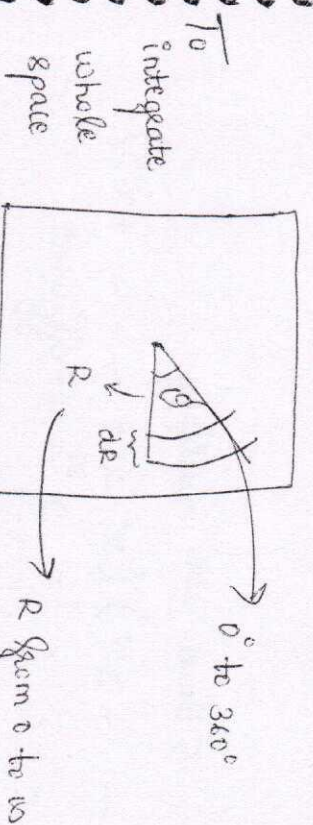
Let  $\frac{x-\mu}{\sqrt{2}\sigma} = t$                        $\therefore \frac{dx}{\sqrt{2}\sigma} = dt$

$$= \int_{-\infty}^{\infty} \frac{1}{\sqrt{\pi}} e^{-t^2} dt = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-s^2} ds \quad \text{--- (2) = I}$$

$$\stackrel{\text{(1)}}{=} I$$

(1)  $\times$  (2)  $I^2 =$

$$\frac{1}{\pi} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} e^{-(s^2+t^2)} ds dt$$



08.02.2018

Assignment Sample Solutions  
11, 19

19.(d)  $2 \leq x_i \leq 10$

$x_1 + x_2 + x_3 + x_4 + x_5 = 21$

$y_1 + y_2 + y_3 + y_4 + y_5 = 11$  (Give 2 to each)

$0 \leq y_i \leq 8$

All solutions,  $a=11, n=5$

$5+11-1C_5 = \underline{\underline{15C_1}}$

(5P2)

$y_i = 9, y_i = 10, y_i = 11$

$5C_1 \times 4C_2 + 5C_1 \times 4C_1$

10 and 1 Either  $y_1, y_2, y_3, y_4$  or  $y_5$  can

be 11 - 5 ways

$\underline{\underline{= 20 \text{ ways}}}$

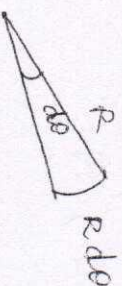
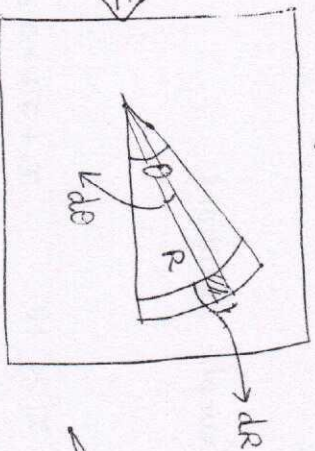
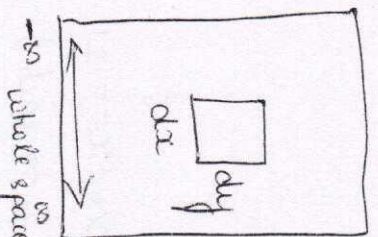
All solutions -  $(y_i = 9 + y_i = 10 + y_i = 11)$

5 times we multiply

$$(x^2 + x^3 + \dots + x^{10}) (x^2 + x^3 + \dots + x^{10}) = x^{21} = \text{co-efficient}$$

OR

Co-efficient of  $x^{21}$  in  $(x^2 + x^3 + \dots + x^{10})^5$



$$I^2 = \int_0^{2\pi} \int_0^{\infty} R e^{-R^2} d\theta dR$$

$$R^2 = u \quad R dR = du/2$$

$$= \frac{1}{2\pi} \int_0^{2\pi} \int_0^{\infty} e^{-u} du d\theta$$

$$= \frac{1}{2\pi} \int_0^{2\pi} (-e^{-u})_0^{\infty} d\theta$$

$$= \frac{1}{2} \int_0^{2\pi} 1 d\theta = \frac{1}{2} [\theta]_0^{2\pi} = \frac{1}{2} (2\pi - 0)$$

$$I^2 = \pi$$

$$I = \sqrt{\pi}$$

$$I = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-t^2} dt = \frac{1}{\sqrt{\pi}} \cdot \sqrt{\pi} = 1$$

$$\int_{-\infty}^{\infty} f(x) dx = 1$$

$$\text{Mean} = \int_{-\infty}^{\infty} x \cdot \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}} dx$$

$$= \int_{-\infty}^{\infty} (x-\mu) \cdot \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}} dx + \int_{-\infty}^{\infty} \mu \cdot \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}} dx$$

$$= 0 + \mu \quad \text{Put } x-\mu = y \quad dx = dy \quad \text{(proved above)}$$

$$\frac{x-\mu}{\sqrt{2}\sigma} = t \quad \frac{dx}{\sqrt{2}\sigma} = dt$$

$$= \int_{-\infty}^{\infty} \frac{t}{\sqrt{\pi}} \cdot e^{-t^2} dt \quad t^2 = y \quad t dt = \frac{dy}{2}$$

$$= \frac{1}{\sqrt{2\pi}\sigma} \int_{-\infty}^{\infty} t e^{-t^2} dt$$

$$= 0$$

$$\text{Variance} = \int_{-\infty}^{\infty} (x-\mu)^2 \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2} dx$$

$$\int uv dx = u \int v dx - \int \frac{du}{dx} \int v dx \Big] dx$$

$$= \int t^2 \cdot e^{-t^2} dt$$

$$= \int t (te^{-t^2}) dt$$

$$= \underline{\underline{0}}$$

$$X(\mu, \sigma^2) \quad f(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

$\downarrow$  mean       $\downarrow$  variance

$Y = ax + b$   $\rightarrow$  new random variable

$$E[Y] = aE[X] + b$$

$$Var = E[Y - E[Y]]^2 = E[ax + b - aE[X] - b]^2$$

$$= E[ax - aE[X]]^2$$

$$= E[a(x - E[X])]^2$$

$$E[ax] = aE[x]$$

$$= a^2 E[x - E[x]]^2$$

$$= \underline{\underline{a^2 \sigma^2}}$$

Standard Normal Distribution  $N(0, 1)$ ;

Convert normal distribution into a new random variable where mean = 0 and variance = 1

$$Y = \frac{X - \mu}{\sigma} \quad = \frac{1}{\sigma} X - \frac{\mu}{\sigma}$$

$$E[Y] = 0$$

$$E[Y - E[Y]]^2 = 1$$

$$E[Y] = aE[X] + b$$

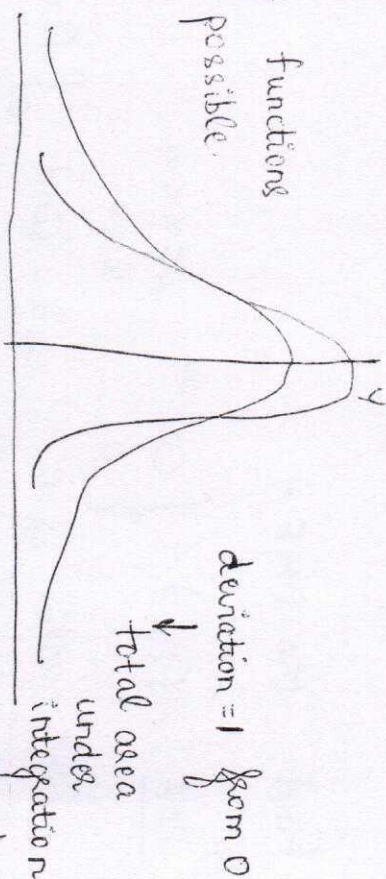
$$= \frac{1}{\sigma} \cdot \mu - \frac{\mu}{\sigma} = \underline{\underline{0}}$$

$$E[Y - E[Y]]^2 = a^2 \sigma^2 = \frac{1}{\sigma^2} \cdot \sigma^2 = \underline{\underline{1}}$$

R.V. Y

$$f(y) = \frac{1}{\sqrt{2\pi}} e^{-y^2/2} dy \quad (\because \mu=0 \text{ \& } \sigma=1)$$

Many functions are possible.



$$\phi(y) = \int_{-\infty}^y \frac{1}{\sqrt{2\pi}} e^{-y^2/2} dy$$

(From table - negative values not given)

$-\infty$  to  $0 = 0.5$  (half of 1)  
(since it is symmetric)

$$\text{Suppose } = \int_a^b \frac{1}{\sqrt{2\pi}} e^{-y^2/2} dy$$

$$\phi(2.18) = 0.9854$$

2.1 and 0.08

row column

Given:

CDF

$$F(b) = \begin{cases} 0 & b < 0 \\ 1/2 & 0 \leq b < 1 \\ 3/5 & 1 \leq b < 2 \\ 1 & b \geq 2 \end{cases}$$

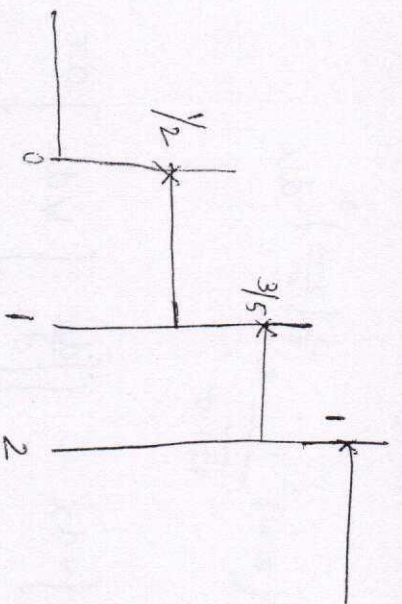
Find the PMF.

2)

$$\text{PDF: } f(x) = \begin{cases} Ce^{-2x} & 0 < x < \infty \\ 0 & x < 0 \end{cases}$$

Find value of  $C$  and find  $\int_{-2}^1 f(x) dx$

①



$$P(0) = 1/2$$

$$P(1) = 3/5 - 1/2 = \frac{6-5}{10} = \frac{1}{10}$$

$$P(2) = 1 - \frac{3}{5} = \frac{5-3}{5} = \frac{2}{5}$$

②

$$\int_0^{\infty} Ce^{-2x} dx = 1$$

$$C \int_0^b e^{-2x} dx = 1$$

$$C = ?$$

$$\int_{-\infty}^{\infty} f(x) dx = 0$$

$$C \left[ \frac{e^{-2x}}{-2} \right]_0^{\infty} = 1$$

$$\frac{-C}{2} [e^{-\infty} - e^{-0}] = 1$$

$$\frac{-C}{2} [0 - 1] = 1$$

$$\frac{C}{2} = 1$$

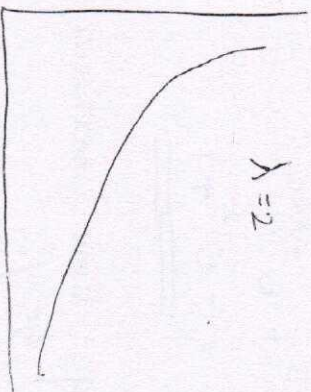
$$C = 2$$

$$-2 \int 2e^{-2x} dx = \frac{-2}{-2} [e^{-2x}]_{-2}^1$$

$$= -1 [e^{-2} - e^4] = \underline{\underline{e^4 - e^{-2}}}$$

16.02.2018

Exponential Distribution:



Time elapsed between 2 events — exponentially distributed  
or interarrival time

$$\text{PDF } f(x) = \begin{cases} \lambda e^{-\lambda x} & x \geq 0 \\ 0 & x < 0 \end{cases}$$

$$E[X] = \int_{-\infty}^{\infty} x f(x) dx = \int_{-\infty}^{\infty} x \cdot \lambda e^{-\lambda x} dx$$

$$= \lambda \int_0^{\infty} x e^{-\lambda x} dx = \lambda \left[ \int_0^{\infty} x \cdot \frac{e^{-\lambda x}}{\lambda} + \left[ \frac{e^{-\lambda x}}{\lambda^2} \right]_0^{\infty} \right]$$

$$= \lambda \left[ \frac{-1}{\lambda} (\infty - 0) \right] + \text{Integrating by parts we get } \underline{\underline{1/\lambda}}$$

$$\text{Variance} = E[X^2] - (E[X])^2$$

$$= \frac{2}{\lambda^2} - \frac{1}{\lambda^2} = \underline{\underline{\frac{1}{\lambda^2}}}$$

$$P(X > 8+t | X > 8) = \frac{P(X > 8+t) \cap P(X > 8)}{P(X > 8)}$$

$$= \frac{P(X > 8+t)}{P(X > 8)}$$

We assume  $X$  is exponentially distributed.

$$= \int_{s+t}^{\infty} \lambda e^{-\lambda x} dx = \lambda \left[ \frac{e^{-\lambda x}}{-\lambda} \right]_{s+t}^{\infty} = \frac{\lambda}{-\lambda} \left[ \frac{e^{-\lambda x}}{-\lambda} \right]_{s+t}^{\infty}$$

$$= \frac{e^{-\lambda(s+t)} - e^{-\lambda(s+t)}}{0 - e^{-\lambda(s+t)}} = \underline{\underline{e^{-\lambda t}}}$$

$$= \frac{e^{-\lambda(s+t)} - e^{-\lambda(s+t)}}{e^{-\lambda s}} = \underline{\underline{e^{-\lambda t}}}$$

$$\begin{aligned}
 P(X > t) &= \int_t^{\infty} \lambda e^{-\lambda x} dx = \lambda \left[ \frac{e^{-\lambda x}}{-\lambda} \right]_t^{\infty} \\
 &= - \left[ e^{-\lambda \infty} - e^{-\lambda t} \right] \\
 &= - (0 - e^{-\lambda t}) \\
 &= e^{-\lambda t}
 \end{aligned}$$

Hence,

$$P(X > 8 + t | X > 8) = P(X > t) = e^{-\lambda t}$$

Memoryless property of exponential distribution.  
 Here, in RHS  $e^{-\lambda t}$  no '8' term is present.  
 Hence, RHS not dependent on LHS  
 Ex: Number of years lived = 8, Number of years will live - not dependent on '8' years.

Job arrives at every 15 seconds on an average.

$$\text{Mean} = \frac{1}{\lambda} = 15 \text{ sec} = \frac{15}{60} = \frac{1}{4} \text{ min}$$

$$\therefore \lambda = 4 \text{ min}$$

To find:  
 Probability of waiting less than 30 seconds.

$$30 \text{ sec} = \frac{30}{60} = \frac{1}{2} = 0.5 \text{ min}$$

$$\begin{aligned}
 P[+ < 0.5] &= \int_{-\infty}^{0.5} \lambda e^{-\lambda x} dx = \int_{-\infty}^0 \lambda e^{-\lambda x} dx + \int_0^{0.5} \lambda e^{-\lambda x} dx \\
 &= \lambda \int_0^{0.5} e^{-\lambda x} dx = \lambda \left[ \frac{e^{-\lambda x}}{-\lambda} \right]_0^{0.5} \\
 &= -e^{-\lambda \times 0.5} + e^{-\lambda \times 0} \\
 &= -e^{-4 \times 0.5} = -e^{-2} + 1
 \end{aligned}$$

Maximum waiting time between two jobs with confidence 95%.

↓  
 Probability of getting next job = 0.95

$$P[+ < t] = 0.95$$

$$\int_0^t \lambda e^{-\lambda x} dx = 0.95$$

$$\lambda \left[ \frac{e^{-\lambda x}}{-\lambda} \right]_0^t = 0.95$$

$$\Rightarrow -e^{-\lambda t} + e^{-\lambda \times 0} = 0.95$$

$$1 - e^{-4t} = 0.95$$

In a call center, calls arrive at an average 12 per hour. Find the probability that a call will occur in next 5 mins, given that already waited for 10 mins.

Given:  $\frac{1}{\lambda} = 12/hr = \frac{12}{60} = \frac{1}{5}/min$

$\therefore \lambda = 5 \text{ min}^{-1}$  (Interarrival time)

$$P[T > 5+10 | T > 10] = P[T > 5] = \int_5^{\infty} \lambda e^{-\lambda x} dx$$

$$= \lambda \left[ \frac{e^{-\lambda x}}{-\lambda} \right]_5^{\infty} = 0 + e^{-\lambda \times 5} = e^{-25}$$

( $\because \lambda = 5$ )

Markov Inequality:  $X$  is R.V (distribution is not known).  $X$  is non-negative. We know  $E[X]$  and Variance

$$E[X] = \int_{-\infty}^{\infty} x f(x) dx = \int_{-\infty}^a x f(x) dx + \int_a^{\infty} x f(x) dx$$

( $\int_{-\infty}^a$  is not known)

2nd kind:  $P[X > a] = \int_a^{\infty} f(x) dx$

$$E[X] \geq \int_a^{\infty} x f(x) dx$$

(Since  $\int_a^{\infty} x f(x) dx$  is +ve)

$$E[X] \geq a \int_a^{\infty} f(x) dx$$

$$E[X] \geq a \cdot P[X > a]$$

$$\therefore P[X > a] \leq \frac{E[X]}{a}$$

20-02-2018

Chebyshev inequality:  $X$  is non-negative R.V with  $\mu, \sigma$

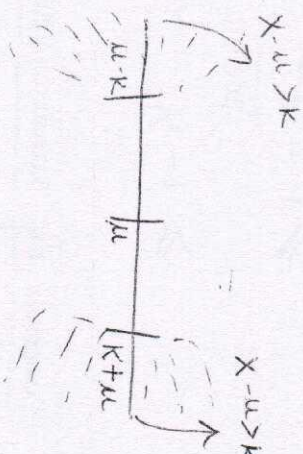
$$P\{|X - \mu| \geq k\} \leq \sigma^2 / k^2$$

( $\{X - \mu\}^2 \geq k^2$  both are same)

Apply Markov inequality

$$\leq \frac{E[(X - \mu)^2]}{k^2}$$

$$\leq \frac{E[(X - \mu)^2]}{k^2} \leq \frac{\sigma^2}{k^2}$$



Post office handles on an average 1000 letters per day. Variance = 2000. What is the probability that Post office will handle more than 2000 letters tomorrow?

(RV)

X: Denotes no of letters handled by the post office

$P\{X > 2000\} \rightarrow$  To find

$$P\{X > 2000\} \leq \frac{E[X]}{2000} \leq \frac{1000}{2000} \leq \underline{\underline{\frac{1}{2}}}$$

2)

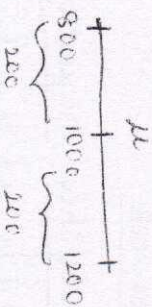
Probability that post office will handle letters b/w 800 and 1200.

$$P\{|X - 1000| \leq 200\}$$

$$= 1 - P\{|X - 1000| \geq 200\}$$

$$\geq 1 - \frac{200}{200^2} \geq 1 - \frac{2000}{200^2} \geq 1 - \frac{2000}{200 \times 200}$$

$$\geq 1 - \frac{1}{10} \geq \underline{\underline{\frac{9}{10}}}$$



Function of Random Variable:

Discrete:

Given PMF of  $X \rightarrow$  To find PMF of  $f(X)$  ( $E(X^2)$ )

$X: P_X(0) = 0.2, P_X(1) = 0.5, P_X(2) = 0.3 \rightarrow$  3 discrete points

To find: PMF of  $X^2$  ( $Y = X^2$ )

$X = \{0, 1, 2\}$   $Y = \{0, 1, 2^2 = 4\}$

$P_Y(0) = 0.2, P_Y(1) = 0.5, P_Y(4) = 0.3$

$Y: 5 \rightarrow \{0, 1, 4\}$

$$\text{Mean} = \frac{0 \times 0.2 + 1 \times 0.5 + 4 \times 0.3}{0.2 + 0.5 + 0.3} = \frac{0.5 + 1.2}{1} = 1.7$$

Continuous:

Given PDF of  $X$ , find out PDF of  $f(X) = X^2$

$Y = X^2$

Find CDF for  $Y = P[Y \leq a] = F(a) = \int_{-\infty}^a f(x) dx$

Then, PDF for  $Y = f(a) = \frac{d}{da} [F(a)]$

Let  $X$  be a RV with PDF  $f(x) = \begin{cases} \frac{3}{2}x^2 & -1 \leq x < 1 \\ 0 & \text{otherwise} \end{cases}$

Find the PDF of  $X^2$ .

Let  $X^2 = Y$

CDF for  $Y = F(a) = P[Y \leq a] = P[X^2 \leq a]$

$= P\{-\sqrt{a} \leq X \leq \sqrt{a}\} = P\{0 \leq X \leq \sqrt{a}\} + P\{0 \leq X \leq \sqrt{a}\}$

$= P\{-\sqrt{a} \leq X \leq 0\} + P\{0 \leq X \leq \sqrt{a}\}$

$$= \int_{-\sqrt{a}}^0 \frac{3}{2}x^2 dx + \int_0^{\sqrt{a}} \frac{3}{2}x^2 dx$$

Case 1: Let  $-a < a < 1$

$$= \frac{3}{2} \cdot \left[ \frac{x^3}{3} \right]_{-\sqrt{a}}^0 + \frac{3}{2} \cdot \left[ \frac{x^3}{3} \right]_0^{\sqrt{a}}$$

$$= \frac{1}{2} [0^3 - (-\sqrt{a})^3] + \frac{1}{2} [(\sqrt{a})^3 - 0^3]$$

$$= \frac{1}{2} \times a^{3/2} + \frac{1}{2} \times a^{3/2} = a^{3/2}$$

$$\therefore \underline{\underline{F(a) = a^{3/2}}}$$

$$\text{PDF } f(a) = \frac{d}{da} [F(a)] = \frac{d}{da} (a^{3/2})$$

$$= \frac{3}{2} a^{3/2-1} = \underline{\underline{\frac{3}{2} a^{1/2}}}$$

negative values  
↓  
not allowed for  $\sqrt{a}$

Case 2:  $a > 1$

$$= -1 \int_{-1}^0 \frac{3}{2} x^2 dx + \int_0^1 \frac{3}{2} x^2 dx$$

$$= \frac{3}{2} \left[ \frac{x^3}{3} \right]_{-1}^0 + \frac{3}{2} \left[ \frac{x^3}{3} \right]_0^1$$

$$= \frac{1}{2} (0 - (-1)^3) + \frac{1}{2} [1^3 - 0]$$

$$F(a) = \frac{1}{2} + \frac{1}{2} = \underline{\underline{1}}$$

$$f_Y(a) = \frac{d}{da} [F(a)] = \frac{d}{da} (1) = 0 \quad a > 1$$

$$f_Y(a) = \begin{cases} \frac{3}{2} a^{1/2} & 0 < a < 1 \\ 0 & a > 1 \end{cases}$$

Proposition: (To find mean)

X: discrete

$$E[g(x)] = \sum g(x) \text{pmf}(x)$$

No need to find pmf of  $g(x)$  to

find  $E[g(x)]$

X: continuous

$$E[g(x)] = \int g(x) \underbrace{f(x)}_{\text{PDF of } X} dx$$

21.02.2018

X is uniform RV over  $(0,1)$ . Find the PDF of  $X^3$ .

$$\text{PDF} = f(x) = \begin{cases} 1 & 0 < x < 1 \\ 0 & \text{otherwise} \end{cases}$$

Let  $X^3 = Y$

$$\text{CDF} = F(a) = P[Y \leq a] = P[X^3 \leq a] = P[X \leq a^{1/3}]$$

$$= \int_0^{a^{1/3}} 1 dx = [x]_0^{a^{1/3}} = a^{1/3}$$

$$\text{PDF} = \frac{d}{da} (F(a)) = \frac{d}{da} (a^{1/3})$$

$$f(a) = \frac{1}{3} a^{1/3-1} = \underline{\underline{\frac{1}{3} a^{-2/3}}}$$

$$f_Y(a) = \begin{cases} \frac{1}{3}a^{-4/3} & 0 < a < 1 \\ 0 & \text{otherwise} \end{cases}$$

or

$$f_Y(x) = \begin{cases} \frac{1}{3}x^{-4/3} & 0 < x < 1 \\ 0 & \text{otherwise} \end{cases}$$

JOINT DISTRIBUTED RV :  $X$  and  $Y$

Discrete :  $X$  &  $Y \rightarrow RV$

$$\text{Joint PMF : } P(X=x, Y=y) = P(x, y)$$

$\downarrow$  To get value of  $\underline{X=x}$ , sum all ' $y$ ' values  
1 value all values

$$P_Y(y) = \sum_x P(x, y)$$

Cumulative :

$$F(a, b) = P(X \leq a, Y \leq b)$$

$$F_X(a) = P\{X \leq a\} \rightarrow Y \text{ can be anything}$$

$$= P\{X \leq a, Y \leq \infty\}$$

$$F_Y(b) = P\{Y \leq b\}$$

$$= P\{X \leq \infty, Y \leq b\}$$

306117001 - Naveen Ranjan  
3069017051 - Gourya Bhattachik

406917051 - Nareatta M.  
406917053 - Haxikhaan R.  
406117005 - K. Sa prabakaran Kumar  
406117003 - K. Sreenivasulu  
406117001 - Randive Krupal Dhanraj

1. Cryptography Theory & Practice - 3rd edition  
Douglas R. Stinson

2. Men Bo Mao

3. Cryptography & N/w Security -  
Behrouz A. Forouzan & Debdeep Mukhopadhyay

4. William Stallings

